

AD-A236 549



DTIC

RECEIVED

JUN 11 1991

2

NAVAL WAR COLLEGE
Newport, R. I.

C4 INTEROPERABILITY: FACT OR FICTION?

by

Judith C. Shaw

Major USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: Judith C. Shaw

11 February 1991

Paper directed by
Colonel Theodore L. Gatchel, USMC
Chairman, Department of Operations



A version for	
1.1.1.1	<input checked="" type="checkbox"/>
1.1.1.2	<input type="checkbox"/>
1.1.1.3	<input type="checkbox"/>
1.1.1.4	<input type="checkbox"/>
by	
Date	
Approved	
Date	
A-1	



REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED		1b. RESTRICTIVE MARKINGS	
2a. SECURITY CLASSIFICATION AUTHORITY		3. DISTRIBUTION/AVAILABILITY OF REPORT DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.	
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE			
4. PERFORMING ORGANIZATION REPORT NUMBER(S)		5. MONITORING ORGANIZATION REPORT NUMBER(S)	
6a. NAME OF PERFORMING ORGANIZATION OPERATIONS DEPARTMENT	6b. OFFICE SYMBOL (If applicable) C	7a. NAME OF MONITORING ORGANIZATION	
6c. ADDRESS (City, State, and ZIP Code) NAVAL WAR COLLEGE NEWPORT, R.I. 02841		7b. ADDRESS (City, State, and ZIP Code)	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c. ADDRESS (City, State, and ZIP Code)		10. SOURCE OF FUNDING NUMBERS	
		PROGRAM ELEMENT NO.	PROJECT NO.
		TASK NO.	WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) C4 INTEROPERABILITY: FACT OR FICTION? (v)			
12. PERSONAL AUTHOR(S) JUDITH C. SHAW, MAJOR, USMC			
13a. TYPE OF REPORT FINAL	13b. TIME COVERED FROM TO	14. DATE OF REPORT (Year, Month, Day) 910211	15. PAGE COUNT 29
16. SUPPLEMENTARY NOTATION A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.			
17. COSATI CODES		18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)	
FIELD	GROUP	SUB-GROUP	
19. ABSTRACT (Continue on reverse if necessary and identify by block number) Joint C4 interoperability is examined through a case study analysis of Cobra Gold-90. With the proliferation of new and changing technologies, interoperability problems continue to plague commanders, and are worsening as equipment becomes more complex to operate. Interoperability can be achieved with adequate planning, but the cost in equipment required, fuel, transportation, personnel, and planning time shows that true interoperability is not yet a fact. What is needed is sensible organization, implementation, and verification of planned, researched, and tested standards, and adequate guidance at the operational level. Jointness must be emphasized at every level. DOD must redefine its decentralized management structure and clearly define joint requirements under the supervision of one agency.			
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS		21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED	
22a. NAME OF RESPONSIBLE INDIVIDUAL CHAIRMAN, OPERATIONS DEPARTMENT		22b. TELEPHONE (Include Area Code) 841-3414	22c. OFFICE SYMBOL C

Abstract of
C⁴ INTEROPERABILITY: FACT OR FICTION?

Joint C⁴ interoperability is examined through a case study analysis of Cobra Gold-90. With the proliferation of new and changing technologies, interoperability problems continue to plague commanders, and are worsening as equipment becomes more complex to operate. Interoperability can be achieved with adequate planning, but the cost in equipment required, fuel, transportation, personnel, and planning time shows that true interoperability is not yet a fact. What is needed is sensible organization, implementation, and verification of planned, researched, and tested standards, and adequate guidance at the operational level. Jointness must be emphasized at every level. DOD must redefine its decentralized management structure and clearly define joint requirements under the supervision of one agency.

TABLE OF CONTENTS

CHAPTER	PAGE
ABSTRACT	11
I INTRODUCTION	1
II BACKGROUND	3
III COBRA GOLD-90: A CASE STUDY	
Exercise Overview	5
Exercise Objectives	6
System Architecture	6
Combined/Joint Planning	10
Exercise Interoperability Problems	12
IV ANALYSIS/RECOMMENDATIONS FOR JOINT INTEROPERABILITY	
Doctrine	16
Planning	17
Equipment	19
V CONCLUSION	23
BIBLIOGRAPHY	25

C4 INTEROPERABILITY: FACT OR FICTION?

CHAPTER I

INTRODUCTION

Command, Control, Communications, and Computers (C⁴), and interoperability have been uneasy and often estranged partners since the first uses of electronic equipment as a means of exercising tactical control of military forces. With the proliferation of new and changing technologies, interoperability problems continue to plague commanders, and are actually worsening as equipment becomes more complex to operate. JCS Pub 1-02 defines interoperability as :

1. (DOD, NATO) The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.
2. (DOD) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly....¹

This paper will examine joint C⁴ interoperability issues through the use of a case study analysis of Cobra Gold-90 (CG-90). This exercise is especially appropriate for study because it involved a combined/joint staff which worked together for several months of planning prior to the exercise, and because it encountered the problems of using service-unique equipment that could not interoperate with other equipment.

¹ U.S. Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington: 1989), p. 49.

This paper will also emphasize that most of the work done in achieving interoperability deals with definition 2 above, the procurement of compatible equipment between the services. I would submit that the most vital, and the most overlooked, part of interoperability is the broader meaning implied in definition 1. Definition 1 also encompasses the ability of units to effectively operate together, not just the interoperability of equipment. With the rapid technological changes occurring, equipment fixes are relatively short-term. What is needed is functional interoperability, a long-term interoperability of doctrine and procedures, and a lack of parochialism among the services. Guidance in this area from JCS and other agencies is sadly lacking, in spite of a congressional mandate directing joint interoperability. Until sufficient emphasis is placed in this area, joint interoperability problems will continue to complicate military operations.

Throughout the paper the terms Command and Control (C²), Command, Control, and Communications (C³), and Command, Control, Communications, and Intelligence (C³I) are cited from various sources. I chose the more inclusive C⁴ because there are many interoperability problems dealing with computers. I did not include intelligence, which is not within the scope of this paper. These terms are different iterations of the same concept, and for the purpose of this paper, may be used interchangeably.

CHAPTER II

BACKGROUND

The requirement for joint interoperability in C⁴ systems has been recognized since World War II, when allied forces were unable to coordinate operations due to different pieces of communication equipment. The problem reoccurred in the Korean War. In Vietnam, Air Force units tasked to provide close air support to Army units could not talk because the Air Force had Ultra High Frequency (UHF) and the Army had Very High Frequency (VHF) radios. In the more recent 1983 Grenada operation, dissimilar equipment, codes, keylists, and procedures prohibited Army, Marine Corps, and Navy components from communicating, and even caused friendly fire from air components to ground units. A review of the Joint Uniform Lessons Learned System (JULLS) data base shows that C⁴ interoperability problems are still an integral part of nearly all joint exercises.

Many attempts have been made to resolve the problem. The Joint Tactical Command, Control, and Communications Agency (JTC³A), established in 1984, was designed to solve interoperability problems in DOD and to develop standards and specifications for joint and combined operations. DOD interoperability directives 4630.5 of 28 January 1967, revised in 1985, and 5154.28 of 5 July 1984 have yet to make an impact. Joint service procurement programs, such as The Tri-Service Tactical Communications Program (TRI-TAC), Joint Interoperability

of Tactical Command and Control Systems (JINTACCS), and the Joint Tactical Information Distribution System (JTIDS) have not provided much interoperable equipment after nearly twenty years in some cases. The Defense Reorganization Act of 1986 (Public Law 99-433), aimed at streamlining the services, eliminating interservice rivalry, and promoting jointness, has yet to significantly influence C⁴ interoperability. The latest attempt is the Defense Communication Agency's (DCA's) center for C³I Standards, which manages an on-line computer Interoperability Decision Support System (IDSS), with over 800 worldwide users. Additional agencies and departments in JCS, DOD, and individual services are also addressing joint interoperability, but the work being done is not resulting in published standards and guidance which can easily be adapted to joint operational planning. Most often planners at the operational level do not have access to the IDSS or published standards for interoperability, or the means to implement them.

CHAPTER III

COBRA GOLD-90 : A CASE STUDY

EXERCISE OVERVIEW

CG-90 was a combined/joint exercise conducted in the Kingdom of Thailand from 23 April to 15 June 1990. The exercise used a Combined/Joint Task Force (CJTf) and Army Forces (ARFOR), Navy Forces (NAVFOR [afloat] and NAVFORTHAI [ashore]), Air Force Forces (AFFOR), Marine Corps Forces (MARFOR), and Combined/Joint Special Operation Forces (CJSOTF), which were all integrated with Thai/US combined staffs. In addition, there was an Exercise Support Group and Exercise Controllers.

The joint staff was formed in September 1989 with a nucleus from the 1st Marine Expeditionary Brigade, Kaneohe Bay, Hawaii, and component members from on-island Hawaii commands. This greatly facilitated planning, as weekly staff meetings were held for several months prior to the exercise to supplement the three planning conferences held.

The exercise itself was conducted in three phases: 1) Cross Training Phase, from 1 to 18 May, where Thai/US forces conducted classes and training together at all exercise locations, 2) Command Post Exercise (CPX), 14 to 18 May, an extensive computer-interactive war game involving all component commands, and 3) Field Training Exercise (FTX), from 26 May to 3 June, an intensive Thai/US combined/joint air, land, maritime, amphibious, and special operations scenario-driven exercise. An amphibious

demonstration and air demonstration preceded the FTX.

EXERCISE OBJECTIVES

An exercise objective was "to improve Thai/US combat readiness and combined/joint interoperability," and to "manage and maintain reliable, interoperable, and secure command, control and communication systems."²

In an effort to accomplish these objectives, the J6 staff established two primary goals: 1) to compose the joint J6 staff section equally between the services, and 2) to source equipment equally from all the services. The J6 staff was eventually composed equally of Air Force, Army, and Marine Corps personnel. In addition, Thai counterparts, primarily Air Force and Army, comprised the combined staff. Out-of-theatre connectivity was engineered with Air Force, Marine Corps, and Navy equipment. In-theatre communications was provided by Air Force and Marine Corps equipment. Component commands provided their own equipment, with Marine Corps augmentation to ARFOR, NAVFOR, CJSOTF, and Thai units. Thai equipment was used at CJTF HQ.

SYSTEM ARCHITECTURE

It became obvious in the planning process that interoperability of equipment would be a major problem. An

² CJTF Cobra Gold-90 Explan 1-90, p. 1.

exercise constraint imposed from the outset was the validation of the Enhanced Crisis Management Capability (ECMC), a one-of-a-kind CINCPAC communication system that had never been deployed. The ECMC consists of a standard Air Force "Jackpot" system of High Frequency (HF), Super High Frequency (SHF), UHF, and VHF radios which has been "enhanced" with a Ground Mobile Forces (GMF) SHF satellite terminal, and multiple computer workstations which are remoted to individual staff sections for on-line message processing and mapping. A staff training session was held at Marine Corps Air Station, Kaneohe Bay, Hawaii, prior to deployment to familiarize the staff with workstation operation.

The ECMC is a large system, requiring four C-141 sorties to transport. It has multiple generators requiring two different types of fuel. In addition, the GMF terminal is not compatible with any of the other Air Force, Marine Corps, or Navy equipment used in the exercise. The ECMC provided the CJTF HQ with DCS AUTODIN connectivity through NAVCAMS EASTPAC (Wahiawa, Hawaii), and a direct link with USCINCPAC HQ. Although not originally identified, it also provided a Worldwide Military Command and Control System (WWMCCS) termination, a secure teleconferencing capability to USCINCPAC, and some single channel radio capability. The DCS entry provided record traffic for the CJTF, CJSOTF, AND ARFOR, which were all co-located at ChonBuri, Thailand. What it did not provide was any in-country connectivity to other component commands at different exercise locations, any in-country switching capability, or AUTOVON. To

provide these capabilities, another parallel system was installed at the same location.

This rather complicated system was assembled from several Air Force units in the Philippines and Korea. It also consisted of GMF SHF terminals located at Chonburi (TSC-94A for CJTF, CJSOTF, ARFOR), Korat (TSC-100A for AFFOR), and Samaesan (TSC-94A for MARFOR). The Air Force also provided a Tropospheric Satellite Support Radio (TSSR) system to extend connectivity to NAVFOR at Utapao and established independent DCS entries for Air Force Special Operations Forces (ARSOF) at Lopburi with a TSC-102 (UHF), and Army Special Operations Forces (ARSOF) at Takhli with a TSC-107 (HF). Navy Special Operations Forces operated from Sattahip, and provided their own equipment. This system provided DCS AUTODIN through the TTC-39 switch at Osan AB, Korea, AUTOVON connectivity from Osan and Clark AB DSN switches, and Digital Secure Voice Telephones (DSVT) for AUTOVON. STU-III's were also used extensively throughout the exercise. The hub-spoke arrangement of this system allowed multiple redundancies and altroute in case of system failure at any location.

A third DCS AUTODIN circuit was installed at Chonburi using a Marine Corps TSC-96A, a UHF satellite terminal, and a TTC-38 telephone switch used for in-country telephone switching. The TSC-96A is not interoperable with either of the other two systems (SHF/UHF) and the switch is not interoperable with the Osan switch (digital/analog). Another independent DCS entry established by NAVFOR at Utapao using the Ashore Mobile

Contingency Communication (AMCC) van was also UHF SATCOM. The Thais provided commercial out-of-country and in-country telephone, military in-country telephone, and military on-base telephone. They also had extensive facsimile capability installed on the telephone system.

The communication success during the exercise was unusually high due to the multiple redundancy of systems and detailed Consolidated Alternate Routing Procedures (CARP) instructions provided. AUTODIN entries were terminated in Hawaii, the Phillipines, Guam, and Japan. No failure at any location significantly degraded the system. But exercise success was paid with an exorbitantly high price in the number of sorties required to transport equipment and personnel, the disproportionate number of communicators required (in excess of 200 at CJTF HQ alone), in-country transportation problems (because of large amounts of equipment, and specialized lifting and carrying requirements), and excessive fuel consumption (the CJTF HQ supported three generator farms, one for each major subsystem). The ECMC required unique generators using 400 gal/day of JP-4 and diesel. When the ten single channel radio nets supporting the exercise were added, there were sixteen dedicated satellite channels required, using several different satellites to obtain connectivity. The extreme complexity of the systems, physical engineering, and management of channels could have been avoided if interoperable equipment had been used. In order to have done this, sole service equipment would have been required, which

would have negated a major exercise objective. However, even Air Force equipments did not interoperate with each other and the ECMC, which was not compatible with anything, was directed to be used.

COMBINED/JOINT PLANNING

Interoperability is often addressed only in terms of technical equipment compatibility. This overlooks the equally important functional interoperability which still does not exist between the services. Several examples of planning during CG-90 eliminated potential problems, while others were not solved so easily.

For the first time in CG-90, a combined/joint Automated Communication-Electronics Operating Instruction (ACEOI) was published by the National Security Agency (NSA). This voluminous document contained all the call signs, staff officer suffixes, frequencies and net instructions for all Thai and U.S. component commands down to the squad/individual aircraft/ship level. Putting together this document required extensive coordination with host country agencies to determine authorized frequencies and locations. Hundreds of frequencies were computer sorted and checked for harmonic and cosite interference. This was done by NSA at considerable expense to the exercise budget. In addition, all inputs were required to NSA by 5 January for 15 April publication. This allowed little flexibility for late changes to unit organization. ACEOI's were mailed directly by NSA to

component Classified Material System (CMS) accounts, as they were classified Confidential-RelThai. This presented a problem in distributing to Thai forces, as no CMS account exists in Thailand for direct mailing. CJTF personnel hand-delivered the nearly 60 cartons of ACEOI's to their Thai counterparts. In spite of these problems, the publication of this document was a significant step forward in allowing all exercise participants to interoperate. The amount of time spent during the exercise in resolving frequency problems was minimal.

The same detailed planning was required in the preparation of a workable telephone directory containing all component commands. With a combination of two dissimilar U.S. switching systems, each requiring different dialing instructions, a combination of U.S. telephone instruments including STU-III, DSVT, rotary dial, pulse and tactical telephones, and three completely independent Thai telephone systems, each with their own instruments and instructions, the task of interfacing for maximum interoperability was considerable.

The same type of effort was required in assigning Plain Language Address (PLA) designators to all units who would be receiving message traffic. The list was voluminous. Each unit was then assigned alternate routing which assigned delivery of their messages to an alternate location automatically should their transmission media be inoperable. This was also done at the several ground entry locations so that messages would also be tracked and rerouted in the event of satellite or ground entry

point failure.

Annex K to the OPLAN contained detailed instructions concerning specific equipment to be used on each radio circuit. Particular attention was paid to crypto equipment and key lists to be used. This is traditionally a problem on most joint exercises because of the proliferation of regular keylists, contingency keylists, special unit keylists, and Integrated Communications Security packages (ICP) which are commonly distributed and often confused. Because the Royal Thai Armed Forces does not have CMS equipment and keylists, crypto liaison teams were assigned throughout the exercise. These U.S. teams assigned to Thai units were quite successful in providing interface between the Royal Thai Armed Forces and U.S. Army, Marine, Navy and Special Forces units.

Two additional interoperability issues were directed in the OPLAN. All messages were directed to be in United States Message Text Format (USMTF) and the computer software program was directed to be Enable. USMTF is the message format being standardized throughout the U.S. Armed Forces. Enable is slowly being implemented as the Marine Corps' standard software program. Its advantages are that it is multipurpose (contains word processing, spreadsheet, and database in one program), and it is able to import data from several other word processing programs.

EXERCISE INTEROPERABILITY PROBLEMS

Systems and Technical Control Facilities were established at

CJTF HQ by U.S. Marine Corps communicators from the 7th Communications Battalion, Okinawa, Japan. Marine Corps' doctrine stresses centralized management of resources and personnel. This is contrary to Air Force doctrine, which generally exercises local control. Therefore, the tracking of current circuit status was difficult, even at CJTF HQ. Component commands did not submit Comm Annexes, except for CJSOTF, and equipment status reports were nonexistent. There was no prompt reporting of equipment outage and prompt maintenance and evacuation of equipment was difficult. CJTF did not have effective control of the C⁴ system as a whole. In spite of this, there was a significant sharing of equipment, without which the exercise would not have been successful. At CJTF HQ, the ECMC used a Marine Corps antenna, and generators were shared, as were radios, telephones, and computers. CJSOTF and ARFOR had virtually no equipment, and were completely sourced from other units. An unplanned field hospital and airfield site were incorporated into the system. Marine Corps personnel equipped and operated the communication center at NAVFOR. Air Force units operated major comm nodes at MARFOR and ARSOF. The Thais contributed significantly by providing radios, telephones, and facsimile machines. Generally, personnel were anxious to work together. What was lacking was clear joint planning doctrine. The only source document used in planning, USCINCPAC/CJTF Joint COMMOPLAN of 21 Jun 88, although providing general guidance, was insufficient in addressing specific doctrinal issues.

There was also a problem with message accountability/tracking. ECMC workstations were installed in each staff section at CJTF HQ. This allowed staff members to compose and edit messages on their computer terminals and then automatically send their messages through AUTODIN. It also allowed on-screen review of all outgoing and incoming messages, so a daily readboard was not required. The disadvantages were that messages with incomplete or wrong PLA's were rejected and sometimes lost. The exact USMTF message format specified for use could not be programmed into the computers. Training the CJTF staff and component commands in the workarounds required for ECMC acceptance proved to be nearly impossible. In addition, message accountability was unsatisfactory. There was a Marine Corps-run communication center at CJTF HQ, but with messages being electronically generated and sent, the normal system of tracking from acceptance through transmission to receipt broke down. The frequent failure of the computer workstations in staff sections, even though the staff liked the concept of automation, caused an undue level of frustration.

An interesting example of redundancy in systems occurred in passing the Air Tasking Order (ATO) from the Combined Air Operations Center (CAOC) at Korat to the Joint Force Air Component Commander (JFACC) at Chonburi. This essential message was promulgated every day about 1600 for the next day's missions. The message was lengthy, often requiring an hour or more to transit the AUTODIN system through Osan and Clark. An alternate

computer data network was established between the CJTF and component commands. Using STU-III telephones and Z-186 laptop computers, the classified ATO could be passed within fifteen minutes. The system could pass data quality point-to-point messages, if required, which provided additional redundancy to the communication center. A third option was tactical facsimile, installed over the telephone system. The computer data network was established by sharing STU-III's and computers across service lines.

CHAPTER IV

ANALYSIS/RECOMMENDATIONS FOR JOINT INTEROPERABILITY

DOCTRINE

Interoperability standards are being developed and implemented. However,

the Joint Oversight Council and the National Security Industrial Association independently have concluded that sufficient accountability does not exist in the standards process.... three different assistant secretaries of defense share responsibilities for C³I standards.... Congress' Office of Technology Assessment identified 'the fractionated U.S. decision making process' as a major impediment to achieving interoperability.³

For standardization to work, not just technical standards are needed, but operational and procedural standards as well. The problem is that in the development of these standards, "[t]he process that goes into producing and maintaining the standards used in the field involves dozens of agencies and innumerable technical experts."⁴

In my study of the subject, there is considerable disagreement among military experts about who is really responsible for developing and implementing interoperability standards. The obvious conclusion drawn is that there is no

³ Thomas L. Parrish, "Crafting Standards Eases Communications Conundrum," Signal, November 1990, p. 59.

⁴ A. W. Mitchell, "Reaching NATO C³ Standards," Signal, October 1989, p. 49.

central direction at the national level; no central agency in charge. Thus it is not surprising that confusion and contradiction exist. When this confusion is applied to the operational level of exercise planning, effective coordination is extremely difficult to achieve.

JTC³A has been developing Functional Interoperability Architectures (FIA) and Commander in Chief (CINC) Interoperability Architectures, but these documents are not fully developed, and are generally at too high a level for effective planning at the operator level. In addition, with no effective system to ensure compliance with published directives, few significant improvements will occur.

PLANNING

"Problems caused by having different sets of equipment, communications standards and protocols, and software stem from a 'not invented here' attitude along with a lack of leadership commitment to do more than pay lip service to interoperability."⁵

The biggest advantages realized by the CG-90 staff was forming the joint staff nucleus from one unit, and having several months to plan for and minimize interoperability problems. Staff training sessions considerably increased equipment familiarity

⁵ Leonard H. Perroots, "New Approaches to C³ Interoperability in the Intelligence Community," Signal, September 1988, p. 34.

and competence, and decreased exercise problems, which were mostly identified prior to the exercise. But in an actual contingency, operations planning time may be minimal. For example, in Grenada, C⁴ was totally inadequate, and planning time was very short. Many problems occurred that would have been corrected with proper planning time. This example shows the importance of having standardized joint planning documents for exercise planners, rather than relying on a 'we've always done it that way' attitude that is peculiar to each service. Such joint documents that do exist are usually written for a certain CINC. Forces to support contingency operations do not always come from the same areas. This is what causes confusions with keylists and other documents, which are also often unit or location specific.

Requiring a 90-day lead time to produce an ACEOI does not allow for these short-fuse operations. Most of the planning time is spent coordinating frequency allocations for the geographic area involved. ICP have been developed for interoperability in specific geographic areas, but all units do not hold the ComSec for every contingency location, and often do not have time to order them. ComSec regulations prohibit passing keylists between units holding different accounts, but this is often done in order to achieve interoperability. In CG-90, in spite of detailed and repeated instructions, units arrived without, or with the wrong ComSec packages. The same problems occurred with computer software and hardware.

It is necessary to move more closely to standardization in

procedural issues, such as the uses of computers and computer software, frequencies, call signs, and keylists. Computer programs are available for local ACEOI generation and are used by some units in areas not covered by their NSA-generated ACEOI. But these documents are not authorized by NSA. It is important that some means be made available to expedite the production and distribution of required documents. Local generation with the proper security requirements, or some type of electronic distribution via computer from NSA appears to be a logical solution.

EQUIPMENT

The conference report on the 1986 DOD Authorization Act stated that:

No equipment should be developed to meet the peculiar needs of any one service if that equipment ultimately diminishes the ability of all the services to interoperate. Furthermore, wherever the operational requirements of the services are substantially similar every reasonable effort should be made to achieve commonality in the development and procurement of system components.⁶

Equipment interoperability, although in my opinion not the most critical component, is certainly the most studied aspect of

⁶ U.S. General Accounting Office, Interoperability, DOD's Efforts to Achieve Interoperability among C³ Systems, Report to the Chairman, Legislation and National Security Subcommittee, Committee on Government Operations, House of Representatives (Washington: 1987), p. 21.

C4 interoperability. Yet there are still significant problems in procurement and fielding of service-unique equipments. A good example is the ECMC, which is not only service-unique but also CINC unique (one-of-a-kind). Although providing some desirable characteristics, it is being eliminated as being too expensive, bulky, complicated to operate, and difficult to maintain. Smaller, portable, interoperable equipment can provide most of the same services.

The same situation exists between radio and satellite equipments of the Army, Air Force, Marines, and Navy, where the acquisition process follows the lead-service concept. Add to this the proliferation of off-the-shelf radios, hand-held radios, computers, and computer software programs that are being purchased without going through any DOD procurement process, and the problem multiplies exponentially.

"DOD's inability to achieve interoperability is primarily related to its decentralized management structure which permits each service a large degree of autonomy over its programs."⁷ For example, when the Navy and Air Force developed JTIDS independently, over \$100 million dollars was spent on a system subsequently cancelled because it would not interoperate.⁸

In another example, the Air Force Automatic Communications Precursor and the Army Short-Term Antijam (STAJ), both due for production in 1989, used identical antijam standards in

⁷ Ibid, p. 13.

⁸ Ibid.

development, but scheduled no interoperability testing. Subsequently, contractors discovered that the two systems will not interoperate in the antijam mode. The same problem occurred with the Army and Air Force Automatic Link Establishment (ALE) equipment.⁹

These examples illustrate the fact that the services are continuing independent development of equipment despite DOD interoperability standards. DOD Directive 5000.3 suggests, but does not require, independent interoperability testing before equipment procurement.

IDSS, which mainly serves the acquisition community, should help in standardizing equipment standards, but until enforcement of these standards is achieved, independent contractors and services are likely to pursue their own unique ways of developing equipment. The same enforcement should be applied to equipment not purchased through DOD acquisition channels.

Partially due to frustration caused by long acquisition cycles, and the inability to procure state-of-the-art equipment, millions of dollars per year is being spent by DOD services on equipment that is not interoperable, does not meet military standards, cannot be maintained or repaired, and is often proven unsuitable and discarded. The financial independency of the services, vigorous congressional and military lobbies, and budget debates often overtake sensible procurement planning. With a

⁹ U.S. General Accounting Office, Defense Reorganization. Progress and Concerns at JCS and Combatant Commands, Report to Congressional Requestors (Washington: 1989), p. 1.

decreased military budget, planners will have to be much more conservative in equipment planning and procurement, or interoperability will continue to be a problem between the services.

CHAPTER V

CONCLUSION

In conclusion, joint C⁴ interoperability is certainly possible, and can be achieved with adequate planning. In CG-90, the communications system was highly successful despite dissimilar equipment, and procedural problems were solved prior to the exercise. But the cost of procuring and fielding equipment that is not interoperable, the costs in transportation, personnel and supplies of using it in operations, and the extra time required for planning multiple redundant systems certainly shows that true interoperability is a fiction that is not approaching reality.

The answer lies not in the creation of new agencies, but in sensible organization, implementation and verification of planned, researched, and tested interoperability standards, and the promulgation of adequate guidance to the operational level where the standards will be used in joint operations.

Jointness needs to be emphasized in planning at every level, and services must be formed to cross parochial boundaries in order to achieve cooperation. DOD must redefine its decentralized management structure to more fully meet the needs of its users. As a prerequisite, DOD must also clearly define joint requirements which are centrally enforced by one agency.

"The ultimate test of C² systems interoperability is whether or not battlefield commanders have an accurate and consistent

understanding of the tactical situation."¹⁰ It would be well for all the planners to remember that the true aim of C⁴ interoperability is command and control. If the electronic systems procured to support C² are not interoperable, command and control on the battlefield will be the sacrifice.

¹⁰ A. M. Gray, "Marines Streamline C³I², Merge Interoperability," Signal, November 1989, p. 82.

BIBLIOGRAPHY

- Armed Forces Communications-Electronics Association, NATO C³ Symposium, 26-28 October 1983. NATO and Western Europe C³ National and International Aspects. Washington: AFCEA International Press, 1983.
- Commander, Joint Task Force, Cobra Gold-90. Explan 1-90 (U). 15 February 1990.
- E. W. Communications, Inc. C³I Handbook. Palo Alto, CA: 1986.
- Gray, Alfred M. "Marines Streamline C³I², Merge Interoperability." Signal, November 1989, pp. 81-83.
- Littlebury, F. E. and Braeger, D. K. Invisible Combat: C³CM. A Guide for the Tactical Commander. Washington: AFCEA International Press, 1986.
- McKnight, Clarence E. Control of Joint Forces, A New Perspective. Washington: AFCEA International Press, 1989.
- Mitchell, A. W. "Reaching NATO C³ Standards." Signal, October 1989, pp. 43-49.
- Mockos, Robert E. NATO Tactical Ground C³: Interoperability is Not Enough. Cambridge, MA: Harvard University, 1983.
- Parrish, Thomas L. "Crafting Standards Eases Communications Conundrum." Signal, November 1990, pp. 59-61.
- Perroots, Leonard H. "New Approaches to C³ Interoperability in the Intelligence Community." Signal, September 1988, pp. 31-34.
- Radford, James H. "C³ Challenges in the U.S. Central Command." Signal, December 1989, pp. 49-53.
- Rockwell, James M., ed., Tactical C³ for the Ground Forces. Washington: AFCEA International Press, 1987.
- Stutz, Darvel C. and Brooks, Michael E. "Architectures for C² Interoperability." Signal, November 1989, pp. 85-88.
- Tardy, J. E. "Communication by Formatted Messages to meet C³I Interoperability Needs." Signal, October 1988, pp. 59-62.
- Technical Communications Corporation. Compatibility among Command and Control Systems in Joint Environments. Submitted to Office of Naval Research. Washington: 1966.

- U.S. Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02. Washington: 1989.
- U.S. General Accounting Office, Defense Reorganization. Progress and Concerns at JCS and Combatant Commands. Report to Congressional Requesters. Washington: March 1989.
- U.S. General Accounting Office, Interoperability. DOD's Efforts to Achieve Interoperability among C³ Systems. Report to the Chairman, Legislation and National Security Subcommittee, Committee on Government Operations, House of Representatives. Washington: April 1987.
- Whigham, John A. "Communications for Deployments and Contingencies." Signal, March 1989, pp. 45-51.